

---

# Sicherheits-Whitepaper: Selbstverpflichtung von OCLC zu sicheren Bibliotheksdiensten

## Inhalt

|  |    |
|--|----|
| Grundsätzliche Informationen.....  | 2  |
| I. Informationssicherheit und Unternehmens-Risikomanagement.....             | 4  |
| A. Konzernrichtlinien von OCLC.....  | 5  |
| B. Datenklassifizierung und -kontrolle .....                                 | 5  |
| II. Physische und Umgebungskontrollen.....                                   | 6  |
| III. Logische Zugangskontrollen.....   | 7  |
| IV. Technische Sicherheitskontrollen.....                                    | 7  |
| A. Sicherheit von Netzwerken.....  | 8  |
| B. Sicherheit des Betriebssystems .....                                      | 8  |
| C. Sicherheit von Anwendungen .....  | 8  |
| D. Verhinderung von Malware .....  | 8  |
| E. Löschung sensibler Daten .....  | 9  |
| V. Systementwicklung und -pflege.....  | 9  |
| VI. Reaktion, Benachrichtigung und Behebung bei Störfällen .....             | 9  |
| VII. Backup, Disaster Recovery (Notfallsystem) und Geschäftskontinuität..... | 10 |
| VIII. Compliance .....   | 10 |
| A. Gesetzlicher Zugang zu Informationen .....                                | 10 |
| B. Datenschutz.....  | 10 |
| IX. Schlussbemerkung.....  | 11 |

## Grundsätzliche Informationen

OCLC (Online Computer Library Center) ist ein weltweiter Bibliotheksverbund, der seit 1967 im Eigentum seiner Mitglieder ist und von ihnen geführt und getragen wird.

OCLC führt Bibliotheken in einem globalen Netzwerk zusammen, um das globale Wissen zu verwalten und auszutauschen und um eine Gemeinschaft zu bilden, die sich den Werten des Bibliothekswesens verpflichtet fühlt: Zusammenarbeit, gemeinsame Nutzung von Ressourcen und allgemeiner Zugang. Die Partnerschaft von OCLC mit den einzelnen Bibliotheken erstreckt sich auf die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten jeder Bibliothek und ihrer Nutzer. OCLC ist den branchenführenden Sicherheits- und Interoperabilitätsgrundsätzen verpflichtet, einschließlich freier Verbindungen und Unterstützung von Standards und Datenübertragbarkeit, die den Anforderungen der Bibliotheksgemeinschaft und ihrer Nutzer gerecht werden. OCLC bietet eine mehrschichtige Sicherheit auf der Grundlage der ISO 27001:2005, Standard für Informationssicherheits-Managementsysteme. Das ISO 27001 Informationssicherheits-Managementsystem (ISMS) von OCLC ist auf unsere ISO 9001:2000 zertifizierten Qualitätsprozesse abgestimmt. OCLC besitzt ISO 9001 und ISO 27001 Zertifizierungen von der Lloyds Quality Registration Assurance.

### *Informationssicherheit und Unternehmens-Risikomanagement*

- OCLC hat ein Informationssicherheits-Managementsystem in Übereinstimmung mit ISO/IEC 27001:2005.
- Fachpersonal zertifiziert in Informationssicherheit, Fachleute für Prüfung von Informationstechnologie (IT) und - und Informationstechnologie-Prüfungsexperten und ein Fachmann, der sich in Vollzeit der betrieblichem Kontinuitäts- und Notfallplanung beschäftigt.

### *Physische und Umgebungskontrollen*

Jedes OCLC-Rechenzentrum verfügt über folgende Kontrollen:

- Rund um die Uhr besetzter Wachdienst
- Kontrollen verhindern unbefugten Zugang zum Rechenzentrum
- Alle Türen, einschließlich cages (Käfige) sind mit Transponder-Karten oder biometrischen Handgeometrie-Lesegeräten gesichert
- Erfassung des gesamten Rechenzentrums, einschließlich der cages (Käfige), durch Videoüberwachungsanlagen (CCTV) mit Digitalkameras und angeschlossenem Archivierungssystem
- Die Videoüberwachungsanlage ist mit Zugangskontrolle und Alarmsystem verbunden
- Bewegungsmelder für Beleuchtung und Videoüberwachung
- Alle Geräte werden bei Eingang geprüft/kontrolliert
- Besucher werden bei Eintritt auf ihre Identität kontrolliert und in Fällen gemeinsamer Nutzung zu ihren jeweiligen Zielorten begleitet
- Der Versand- und Warenannahmehbereich ist räumlich von den Stellplätzen der Rechner getrennt
- Die Klimaanlage bietet geeignete Luftführung, Temperatur und Luftfeuchtigkeit für optimale Bedingungen für den Betrieb von Geräten und zur Minimierung der Ausfallzeit im Falle von Gerätestörungen.
- Das Rechenzentrum verfügt über Stromversorgungsanlagen mit eingebauter Redundanz, vollständigen unterbrechungsfreien Stromversorgungs- (UPS-)Systemen mit N+1 Level oder höher und Notstromgeneratoren für den Fall eines lokalen Stromausfalls.
- Redundante Stromverteilungsgeräte (PDUs)
- Alternative Stromerzeugung
- Rauch- und Feuermeldesensoren überall im Rechenzentrum

- Schutz durch automatische Feuermelde- und Feuerbekämpfungsanlagen. Zudem sind überall Feuerlöscher vorhanden

### Logisch Zugangskontrollen

- Die Kommunikation zwischen Anwendungen ist anonymisiert, um die Wahrscheinlichkeit einer unberechtigten Kenntnisnahme zu verringern
- Das Identity and Access Management Module (IDM) sorgt für die Nutzeridentifizierung und das Zugangsmanagement
- Nutzeridentifizierung und Zugangsmanagement
  - Verbindungen zum Endnutzer über SSL 3.0/TLS 1.0, unter Verwendung globaler Step-up-Zertifikate von Thawte, mit denen sichergestellt wird, dass unsere Nutzer eine sichere Verbindung von ihren Browsern zu unserem Dienst haben\*
  - Die Sitzungen der einzelnen Nutzer werden, unter Verwendung von XML-verschlüsselter Authentifizierungs- und Autorisierungsinformationen über Security Assertion Markup Language (SAML) 3.0\* identifiziert und bei jeder Transaktion erneut geprüft

*\* Je nach den genutzten besonderen Diensten*

### Technische Sicherheitskontrollen

- Mit dem Internet über redundante, unterschiedlich geführte Verbindungen von mehreren Internetdienstleistern verbunden, die von mehreren Präsenzpunkten verschiedener Telekommunikationsdienstleister bereitgestellt werden
- Perimeter-Firewalls und Edge-Router sperren nicht-autorisierte Protokolle
- Interne Firewalls trennen den Traffic zwischen den Anwendungs- und den Datenbankebenen
- Load-Balancer stellen Proxies für den internen Traffic bereit
- OCLC verwendet eine Vielzahl von Methoden zur Verhinderung, Erkennung und Beseitigung von Malware
- Darüber hinaus werden regelmäßig unabhängige Sicherheitsbewertungen durch Dritte durchgeführt
- Das Informationssicherheitspersonal von OCLC überwacht Benachrichtigungen aus verschiedenen Quellen und Meldungen aus internen Systemen, um Bedrohungen zu erkennen und zu bewältigen

### Systementwicklung und -pflege

- OCLC testet den gesamten Code vor der Freigabe auf Sicherheitsschwachstellen und prüft sein Netzwerk und seine Systeme regelmäßig auf Schwachstellen
- Bewertung von Netzwerkschwachstellen
- Ausgewählte Penetrationstests und Code-Überprüfung
- Überprüfung und Tests der Sicherheitskontrollmechanismen

### Backup, Disaster Recovery und Geschäftskontinuität

- Der OCLC-Dienst erstellt im jeweiligen Rechenzentrum eine lokale Echtzeit-Datenkopie auf Festplatten
- Durch Notfallwiederherstellungstest (Disaster-Recovery-Tests) werden unsere geplanten Wiederherstellungszeiten und die Richtigkeit und Vollständigkeit der Kundendaten kontrolliert
- Alle Daten werden täglich auf Band gesichert, verschlüsselt und außerhalb des Standorts in einer sicheren Einrichtung aufbewahrt.
- Die Backups werden über sichere Verbindungen in ein Archiv für sichere Bänder kopiert.

### Reaktion, Benachrichtigung und Behebung bei Störfällen

- Managementprozess für Sicherheitsereignisse, die die Vertraulichkeit, Integrität oder Verfügbarkeit der Systeme oder Daten von OCLC beeinträchtigen können

- Das Informationssicherheitsteam von OCLC ist als Vorbereitung auf Vorfälle in der Spurensicherung und im Umgang mit Nachweisen geschult, einschließlich dem Einsatzes externer und eigenentwickelter Tools

### *Einhaltung gesetzlicher Vorschriften und Konzernrichtlinien (Compliance)*

- Personenbezogene Daten von Bibliotheksnutzern können von Dritten nur auf dem Rechtsweg, etwa über Durchsuchungsbefehle, Gerichtsbeschlüsse, Vorladungen, gesetzliche Ausnahmeregelungen oder mit Einwilligung der Nutzer erlangt werden
- OCLC stellt in Zusammenarbeit mit Bibliotheken die Einhaltung nationaler, staatlicher und regionaler Gesetze zur Privatsphäre und zum Datenschutz sicher

## **I. Informationssicherheit und Unternehmens-Risikomanagement**

Das Informationssicherheits-Managementsystem (ISMS) von OCLC legt unsere Verpflichtungen gegenüber unseren Kunden fest. Das Informationssicherheitsprogramm basiert auf ISO/IEC 27001:2005, Empfehlungen der Cloud Security Alliance und allgemein anerkannten Systemsicherheitsgrundsätzen. Das Informationssicherheitsprogramm ordnet Sicherheitsanforderungen drei Bereichen der obersten Ebene zu: Administrative, technische und physische Anforderungen. Die Kriterien in diesen Bereichen bilden die Grundlage für den Umgang mit Sicherheits- und Compliance-Risiken. Ausgehend von den in den Bereichen und ihren Unterkategorien identifizierten Schutzmaßnahmen und Kontrollen orientiert sich das Informationssicherheitsprogramm an den Vorgaben von ISO/IEC27001:2005 "Planen, Ausführen, Prüfen, Umsetzen". Das Sicherheitsprogramm von OCLC ist auf einer mehrschichtigen Sicherheitsstrategie aufgebaut, die eine Kombination aus Präventions- und Aufdeckungskontrollen auf verschiedenen Ebenen von Datenzugriff, -speicherung und -übertragung bietet. Die OCLC-Strategie beinhaltet Folgendes:

- OCLC-Unternehmensgrundsätze
- Datenklassifizierung und -kontrolle
- Personalbezogene Sicherheit
- Physische und Umgebungskontrollen
- Logische Zugangskontrolle
- Betriebliche Sicherheitskontrollen
- Systementwicklung und -pflege
- Disaster Recovery und Geschäftskontinuität
- Management, Benachrichtigung und Behebung von Sicherheitsvorfällen
- Compliance

Zur Erfüllung interner und externer regulierenden Vorschriften hat OCLC eine Reihe von Kontroll- und Sicherheitsverfahren eingerichtet. Diese Verfahren schreiben Transparenz und Überprüfung für Sicherheits-Tools vor, einschließlich Schwachstellen, Logging, Malware-Schutz und Spam-Schutz. OCLC ist sich bewusst, dass Corporate-Governance- und Compliance-Anforderungen komplex sind und sich nach Ländern, Bibliotheksarten und anderen Variablen unterscheiden. Daher harmonisieren wir diese Anforderungen, um eine einheitliche Sicherheitsstrategie auf der Grundlage strengsten Vorgaben zu schaffen.

OCLC beschäftigt ein Informationssicherheitsteam in Vollzeit, das in die OCLC-Abteilung Global Systems & Information Technology eingegliedert ist. Sie besteht aus erfahrenen und zertifizierten Sicherheits-, Prüfungs- und Compliance-Fachleuten mit weit reichenden Kenntnissen in Sicherheitsarchitektur, Anwendungen und Netzwerksicherheit. Dieses Team ist für die Überwachung der perimeter defense systems (ein System zur Abgrenzung des betrieblichen Netzwerkes zum externen Netzwerk z.B. Internet), die Erarbeitung von Sicherheitsüberprüfungsprozessen und die Beratung der strategischen Führungskräfte von OCLC hinsichtlich einer

maßgeschneiderten Sicherheitsinfrastruktur verantwortlich. Das OCLC-Sicherheitsteam übernimmt eine führende Funktion bei der Entwicklung, Dokumentierung und Umsetzung von Sicherheitsgrundsätzen und -standards. Das Team ist verantwortlich für:

- die Überprüfung von Sicherheitsplänen für Netzwerke, Systeme und Dienste von OCLC unter Anwendung von Branchenstandards des Center for Internet Security, der ISACA und des Institute of Internal Auditors,
- die Durchführung von Überprüfungen des Sicherheitskonzepts,
- die Laufende Beratung zu Sicherheitsrisiken in Verbindung mit einem bestimmten Projekt und mögliche Lösungen für Sicherheitsprobleme,
- die Förderung der Einhaltung festgelegter Grundsätze durch routinemäßige Sicherheitsbewertungen und interne Prüfungen,
- die Beauftragung externer Sicherheitsexperten mit der Durchführung regelmäßiger Sicherheitsbewertungen von Infrastruktur und Anwendungen von OCLC,
- die Ausführung eines Schwachstellenmanagementprogramms, mit dessen Hilfe Problembereiche in den Netzwerken, Systemen und Anwendungen entdeckt werden sollen, und Überwachung ihrer Beseitigung,
- die Überwachung verdächtiger Aktivitäten in OCLC-Netzwerken und Befolgung formeller Prozesse zur Reaktion auf Sicherheitsvorfälle, um Informationssicherheitsgefahren schnell erkennen, analysieren und beseitigen zu können

## A. Konzernrichtlinien von OCLC

OCLC ist der Sicherheit aller Daten verpflichtet, die in seinen Informationssystemen gespeichert sind oder sie durchlaufen. Diese Selbstverpflichtung wird im OCLC-Verhaltenskodex bekräftigt. Die Grundlage der Selbstverpflichtung von OCLC auf Sicherheit ist in seinen zentralen Konzernrichtlinien, -Verfahren und Leitfaden niedergelegt, die physische Dienste, Konto-, Daten- und Unternehmensdienste, Netzwerk- und Computersysteme, Anwendungsdienste und Systemdienste behandeln. Diese Richtlinien werden regelmäßig überprüft, um dadurch ihre dauerhafte Relevanz, Effektivität und Richtigkeit sicherzustellen.

Die OCLC-Mitarbeiter sind zu einem Verhalten verpflichtet, das mit den Richtlinien des Unternehmens hinsichtlich Verschwiegenheit, Unternehmensethik, angemessener Nutzung und professioneller Standards übereinstimmt. Bei der Einstellung überprüft OCLC die Ausbildung und vorherige Beschäftigung einer Person und überprüft die internen und externen Referenzen. Soweit nach lokalem Arbeitsrecht oder Gesetzesvorschriften zulässig, kann OCLC auch Vorstrafen-, Bonitäts- und Sicherheitsüberprüfungen durchführen. Der Umfang von Zuverlässigkeitsprüfungen richtet sich nach den Funktionen und den Verantwortlichkeiten der Person. Alle Beschäftigten sind an Geheimhaltungsverpflichtungen in ihrem Anstellungsvertrag gebunden und müssen die Richtlinien im OCLC-Standardhandbuch oder dem lokalen Mitarbeiterhandbuch befolgen. Auf die Geheimhaltung und den Schutz von Kundeninformationen und -daten wird in den Mitarbeiterleitlinien und im Einweisungsprogramm für neue Mitarbeiter besonders hingewiesen.

## B. Datenklassifizierung und -kontrolle

Zur Unterstützung unserer Bibliothekskunden muss die OCLC-Dienstumgebung zusätzlich zu den strengen Vorgaben des OCLC-Managements zahlreiche staatlich vorgeschriebene und branchenspezifische Sicherheitsanforderungen erfüllen. Im Zuge der weiteren Zunahme und Entwicklung der OCLC-Angebote in der Cloud wird mit zusätzlichen Anforderungen gerechnet, die regionale und landesspezifische Datensicherheitsstandards beinhalten könnten. Das OCLC-Sicherheitsteam stellt zusammen mit den Teams für Operation, Produktentwicklung und Servicebereitstellung sicher, dass OCLC die einschlägigen Gesetze (national, regional und lokal), Standards und behördliche Vorschriften einhält. Dazu gehören unter anderem:

- Der Datensicherheitsstandard der Zahlungskartenindustrie (Industrie)

- Die EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) und die Richtlinie 202/58/EG
- Der *Health Insurance Portability and Accountability Act* (USA)
- Der *Family Educational Rights and Privacy Act* (USA)
- Der *Privacy Act 1988* (Australien) und der *Privacy Act 1993* (Neuseeland)
- Der *Personal Information Protection and Electronic Documents Act* (Kanada)
- Der *Federal Information Security Management Act* (National Institute of Standards and Technology (NIST) Special Publication 800-53) (USA)
- Der *Children's Online Privacy Protection Act* (USA)
- Commission of the Sponsoring Organizations of the Treadway Commission - Interne Kontrolle der Finanzberichterstattung (USA)
- Bundesamt für Sicherheit in der Informationstechnik (BSI) Standard 100-1 Managementsysteme für Informationssicherheit (ISMS) (Deutschland)

## II. Physische und Umgebungskontrollen

Sämtliche OCLC Rechenzentren (sowohl eigene Rechenzentren als auch Vertragsrechenzentren) arbeiten mit einer Vielzahl physischer Sicherheitsmaßnahmen. Die in jedem OCLC-Rechenzentrum eingerichteten physischen Standard-Sicherheitskontrollen bestehen aus bewährten Techniken und folgen allgemein anerkannter Industriestandards: speziell konzipierte Zugangskontrollsysteme mit elektronischen Karten, zentrale Videoüberwachung und -aufzeichnung und Sicherheitskräfte. Der Zugang zu Bereichen, in denen Systeme und Systemkomponenten installiert sind oder aufbewahrt werden, ist von Verwaltung (Zentrale) und öffentlichen Bereichen getrennt. Alle Vertragsrechenzentren von OCLC erfüllen dieselben Sicherheitsanforderungen, wie die eigenen Rechenzentren von OCLC. Die Vertragsrechenzentren sind ebenfalls ISO 27001 zertifiziert und verfügen über SSAE-16/IASE-3402 Gutachten von unabhängigen Prüfern. Die Zertifizierungen und Gutachten werden laufend überprüft und wiederholt, um eine Rechtskonformität sicherzustellen.

Der Zugang zu allen Rechenzentrumseinrichtungen ist auf autorisierte OCLC-Mitarbeiter, zugelassene Besucher und zugelassene Dritte, deren Aufgabe der Betrieb des Rechenzentrums ist, beschränkt. Prüfer von OCLC erhalten einmal im Vierteljahr Zugang zu dessen Rechenzentren, um dadurch sicherzustellen, dass nur geeignetes Personal Zugang zu den Rechenzentren hat. Die Rechenzentren von OCLC wurden stabil, fehlertolerant und gleichzeitig wartbar gestaltet.

Die Energie zur Unterstützung der laufenden Tätigkeiten von OCLC stammt aus redundanten Stromversorgungsanlagen. Für jede kritische Komponente im Rechenzentrum werden eine primäre und eine alternative Stromquelle vorgesehen, jeweils mit gleicher Kapazität. Eine unterbrechungsfreie Stromversorgung (UPS) soll bis zur Umstellung auf die Notstromgeneratoren Energie bereitstellen. Die Notstromgeneratoren können genügend Notstrom liefern, um für eine bestimmte Zeit das Rechenzentrum mit voller Kapazität zu betreiben.

Heizungs-, Belüftungs- und Klimaanlage sorgen für eine konstante Betriebstemperatur für Server und andere Computerhardware. Die Kühlung verhindert eine Überhitzung und verringert die Möglichkeit eines Ausfalls der Dienste. Die Klimaanlage im Computerraum werden mit normalen und mit Notstromsystemen angetrieben.

Automatische Feuermelde- und Feuerlöschanlagen tragen dazu bei, Schäden an der Computerhardware zu verhindern. Die Feuermeldesysteme arbeiten mit im Rechenzentrum angeordneten Wärme-, Rauch- und Wassersensoren. Bei Feuer oder Rauchentwicklung löst das Meldesystem akustischen und optischen Alarm aus. Darüber hinaus befinden sich Handfeuerlöcher überall in den Rechenzentren. Die Techniker des Rechenzentrums werden in Brandschutz- und Feuerlöschmaßnahmen geschult, einschließlich der Benutzung von Feuerlöschern.

### III. Logische Zugangskontrollen

OCLC verfügt über umfangreiche Kontrollen und Verfahren zum Schutz der Sicherheit von Daten der Bibliotheksnutzer<sup>1</sup>. Der Zugang für Bibliothekspersonal und Bibliotheksnutzer kann von den meisten Institutionen unter Verwendung kombinierter Modelle wie Shibboleth oder dem LDAP der Institution festgelegt werden. Für den authentifizierten Zugang setzen die Cloud-Angebote des OCLC den Security Assertion Markup Language (SAML) 2.0 XML-basierten Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomains über das Identitätsmanagement- (IDM-)Modul ein. Der Zugang zu sensiblen Daten ist durch eine sichere HTTP (HTTPS) und Secure Socket Layer (SSL) 3.0/Transport Layer Security (TLS) 1.0 Verschlüsselung geschützt. Die OCLC-Anwendungen bieten institutionellen Kunden Möglichkeiten zur Vergabe von Berechtigungen und Vorrechten entsprechend den Funktionen und lokalen Richtlinien zur Aufgabentrennung.

Die Cloud-Anwendungen von OCLC werden in einer mandantenfähigen, verteilten-Umgebung mit logischen Zugangskontrollen zur Beschränkung des Zugriffs zwischen Kunden betrieben. Der Zugang des OCLC-Personals zu Produktionsumgebungen wird ähnlich kontrolliert. Der Administrator-Zugang zu Produktionsdiensten wird über eine zentrale Gruppe festgelegt und kontrolliert. OCLC verwaltet den Zugang zu Ressourcen und Diensten nach dem Prinzip der unbedingt erforderlichen geringsten Rechte. Soweit machbar, werden funktionsbezogene Zugangskontrollen verwendet, um den logischen Zugang speziellen Arbeitsaufgaben oder Verantwortungsbereichen und nicht einzelnen Personen zuzuweisen. Personen mit Zugangsberechtigung für die Anlagen müssen die entsprechenden Methoden anwenden, um Zugang zu erhalten. Für hoch sensible Anlagen ist eine mehrstufige Authentifizierung erforderlich, einschließlich Methoden wie Passwort und Hardware-Token. Durch einen kontinuierlichen Abgleich von Nutzerkonten und Zugangsberechtigungen wird sichergestellt, dass die Nutzung einer Anlage zur Erfüllung der zugewiesenen Aufgaben angemessen und notwendig ist. Accounts, die einen Zugang zu einer bestimmten Anlage nicht mehr benötigen, werden deaktiviert.

### IV. Technische Sicherheitskontrollen

Die Verfügbarkeit eines Defense-in-Depth-Sicherheitskonzepts ist von fundamentaler Bedeutung für die Art und Weise, wie OCLC eine sichere und vertrauenswürdige Computerinfrastruktur bereitstellt. Der Einsatz eines Defense-in-Depth-Sicherheitskonzepts verbessert unsere Kapazität zur Aufdeckung und Verhinderung von Sicherheitsverstößen oder zur Minderung der Auswirkungen eines Sicherheitsvorfalls. Die Anwendung von Kontrollen auf mehreren Ebenen beinhaltet den Einsatz von Präventions- und Aufdeckungskontrollen, die Erarbeitung von Risikominderungsstrategien und die Fähigkeit zur Reaktion auf Angriffe, sobald diese eintreten. Daher konzentrieren sich unsere Informationssicherheitsaktivitäten auf Risiken in der Nähe der Anwendungsebene, wie etwa Objekte, statische oder dynamische Datenspeicher, die virtuellen Maschinenobjekte oder die Laufzeitumgebungen, in denen Transaktionen erfolgen. Risikomanagement und entsprechende Überprüfungen sind dieser dynamischen Umgebung angepasst. OCLC verwendet Prozesse auf der Grundlage seiner langjährigen Erfahrung mit der Lieferung von Diensten im Internet zur Bewältigung dieser neuen Risiken.

Das Informationssicherheitsprogramm von OCLC legt die Standardprozesse und Dokumentationsanforderungen für die laufende risikobezogene Entscheidungsfindung fest. Das Informationssicherheitsteam von OCLC bewertet in Zusammenarbeit mit Systementwicklern, operativem und Kundenunterstützungspersonal Schwachstellen in Systemen und Diensten. Risikobewertungen erfolgen auf mehreren Ebenen und informieren das OCLC-Management über Priorisierungen in Bereichen wie Produktveröffentlichungspläne, Pflege von Richtlinien und Ressourcenverteilung. Zu jedem Produkt gehört eine umfassende Gefahrenbewertung, an die

---

<sup>1</sup> „Daten der Bibliotheksnutzer“ bezeichnet alle Daten im Zusammenhang mit einem Bibliotheksnutzer oder „Klienten“, die dem OCLC von der Bibliothek geliefert werden, einschließlich das Ausleihen von Medien, Bestände, Profile und Bibliothekskontodaten.

sich weitere Überprüfungen im Jahresverlauf anschließen. Diese laufenden Arbeiten konzentrieren sich auf solche Gefahren, die die Verfügbarkeit, Integrität und Vertraulichkeit von Diensten und Daten beeinträchtigen könnten. Durch diesen Prozess priorisiert und steuert OCLC die Entwicklung von Sicherheitskontrollen und damit verbundenen Aktivitäten.

## A. Sicherheit von Netzwerken

Zum Schutz der Netzwerk-Umgebung vor Angriffen von außen setzt OCLC mehrere Abwehrebene ein. Das OCLC-Netzwerkteam führt ein systematisches Management der Netzwerk-Firewalls und der ACL-Vorschriften aus, das Change-Management, Peer-Review und Tests verwendet. Nur autorisierte Dienste und Protokolle, die den Sicherheitsanforderungen von OCLC genügen, dürfen das Unternehmensnetzwerk durchlaufen.

OCLC verwendet mehrere Systeme zur Statusüberwachung von System, Anwendung, Internetseiten und Internetdiensten und zur Information des operativen und des unterstützenden Personals über Probleme, so dass diese möglichst gelöst werden, bevor sie für den Nutzer der OCLC-Systeme spürbar sind. Treten Probleme auf, senden die Systeme auf zahlreichen verschiedenen Wegen Benachrichtigungen an die zuständige Administration. Die Systeme stellen den Betreibern detaillierte Statusinformationen, bisherige Protokolle und Berichte zur Verfügung. Diese Analyse wird mit einer Kombination aus Open-Source und kommerziellen Tools zur Traffic-Erfassung und zur Syntexanalyse durchgeführt. Die Netzwerkanalyse wird durch Prüfung der Systemprotokolle ergänzt, um ungewöhnliches Verhalten, wie etwa unerwartete Aktivität in Accounts ehemaliger Mitarbeiter oder Zugriffsversuche auf Kundendaten, festzustellen.

## B. Sicherheit des Betriebssystems

Die Produktionsserver von OCLC beruhen auf einheitlich verbesserte Windows- und Linux-Betriebssysteme (OS) und Sicherheits-Patches werden durchgängig in der OCLC-Infrastruktur eingesetzt. Das Sicherheitsteam bewertet die Geräte nach Industriestandards, wie etwa den des Center for Internet Security, und verwendet automatische Schwachstellenscanner zur Identifizierung und Behebung von Sicherheitsproblemen vor dem Einsatz in der Produktionsumgebung. OCLC setzt ein Change-Management-System zur Identifizierung, Prüfung und Einsatz kritischer Sicherheits-Patches und -Updates ein, um die Integrität der Betriebssysteme zu erhalten. OCLC hat ein Change-Management-System zur Minimierung der Risiken, die mit der Ausführung nicht autorisierter Änderungen am Aufbau des Produktions-Betriebssystems verbunden sind.

## C. Sicherheit von Anwendungen

Die Sicherheit der Anwendungen ist ein wichtiges Element im Konzept von OCLC zur Sicherung seiner Cloud-Computing-Umgebung. Das OCLC-Sicherheitsteam hat die wichtige Funktion, sicherzustellen, dass Sicherheitsanforderungen definiert werden; Bedrohungen von Anwendungen werden anhand des Open Web Application Security Project (OWASP), der Bedrohungseinstufung des Web Application Security Consortium (WASC) und allgemeiner Schwachstellenerkennung identifiziert. OCLC hat ein Sicherheitsprogramm (Software) installiert, welches von unserer Application Security Working Group gesteuert wird. Gleichzeitig hat OCLC einen Sicherheitsstandard seiner Anwendungen auf Basis der SANS Institute Securing Web Application Technologies (SWAT) und Open Web Application Security Project Top 10 Vulnerabilities festgelegt. Zusätzlich durchlaufen die Anwendungen einen Sicherheitstest und eine Bewertung mit Beseitigung identifizierter Ausnahmeregelungen.

## D. Verhinderung von Malware

Malware stellt ein erhebliches Risiko für die Informationssystemumgebungen von heute dar. OCLC ist sich bewusst, dass ein Malware-Angriff zur Gefährdung von Benutzerkonten, Datendiebstahl und möglicherweise weiterem Zugang zu einem Netzwerk führen kann. Daher nimmt OCLC diese Bedrohungen seiner Netzwerke



und seiner Kunden ernst und wendet eine Vielzahl von Methoden zur Verhinderung, Aufdeckung und Beseitigung von Malware an. Darunter fällt auch der Einsatz kommerzieller Malware-Schutzlösungen auf Unternehmensebene für Server und Endanwender.

## E. Löschung sensibler Daten

Bei der Entsorgung von Datenträgern, die sensible Daten enthalten, durchlaufen sie ein Datenvernichtungsverfahren, bevor sie den Kontrollbereich von OCLC verlassen. Soweit möglich, werden die Datenträger von hierzu berechtigten Personen logischerweise gelöscht. Die Löschung besteht aus einer vollständigen Überschreibung des Laufwerks mit Nullen, gefolgt von einer vollständigen Lesung des Laufwerks, um sicherzustellen, dass der Datenträger leer ist. Kann das Laufwerk aufgrund einer Hardware-Störung nicht gelöscht werden, wird es sicher gelagert, bis es vernichtet werden kann.

## V. Systementwicklung und -pflege

Die von Entwicklungsteams angewandten strengen Sicherheitsverfahren sind im Produktmanagement-Lebenszyklus (PMLC) von OCLC verbindlich vorgeschrieben. Der OCLC-PMLC ist von der Konzeption bis zur Reaktion vollständig in den Produktentwicklungs-Lebenszyklus integriert. Die Konzernleitung von OCLC fördert weiterhin den Auftrag, den PMLC auf die Entwicklungsprozesse von OCLC-Produkten, einschließlich der Lieferung von Online-Cloud-Diensten, anzuwenden.

OCLC unterhält getrennte Umgebungen für Entwicklung, Qualitätssicherung/-prüfung und Produktion. Anwendungsänderungen werden vor der Übernahme in die Produktionsumgebung gründlich getestet, um die Qualität des Dienstes sicherzustellen und Serviceunterbrechungen zu verhindern. Das Änderungsmanagement von OCLC für Netzwerke, Betriebssysteme, Anwendungen und Datenbanken sorgt dafür, dass Änderungen bewertet, vom Management genehmigt und terminiert werden, um Serviceunterbrechungen zu verhindern.

## VI. Reaktion, Benachrichtigung und Behebung bei Störfällen

OCLC verfügt über einen Managementprozess für Störfälle, die die Vertraulichkeit, Integrität oder Verfügbarkeit der Systeme oder Daten von OCLC beeinträchtigen können. Dieser Prozess spezifiziert Vorgehensweisen und die Verfahren zur Benachrichtigung, Eskalation, Schadensminderung und Dokumentation. Die Verfahren von OCLC für den Umgang mit Computerstörfällen sind nach dem NIST-Leitfaden zur Handhabung von Störungen (NIST Special Publication 800-51) strukturiert. Sicherheitsverletzungen<sup>2</sup> werden zeitnah untersucht und die Rechtsabteilung benachrichtigt die betroffenen Institutionen so schnell wie unter den gegebenen Umständen möglich und ohne unzulässige Verzögerung, jeweils in Übereinstimmung mit den legitimen Anforderungen des anwendbaren Gesetzesvollzugs und nach Einsatz aller erforderlichen Maßnahmen zur Ermittlung des Umfangs der Verletzung und zur Wiederherstellung der angemessenen Integrität des Systems.

Das Informationssicherheitsteam ist in der Spurensicherung und im Umgang mit Beweisen zur Vorbereitung eines Ereignisses geschult, einschließlich des Einsatzes externer und eigenentwickelter Tools. Um die rasche Klärung von Sicherheitsvorfällen sicherzustellen, ist das OCLC-Sicherheitsteam weltweit 24 Std./7 Tage erreichbar. Tritt ein Informationssicherheitsvorfall ein, reagiert das OCLC-Sicherheitsteam durch Protokollierung und Priorisierung des Vorfalls entsprechend seinem Schweregrad. Ereignisse mit direkten Auswirkungen auf Kunden werden mit höchster Priorität behandelt. Das OCLC-Sicherheitsteam wird erforderlichenfalls hinsichtlich nachträglicher Ermittlungen beratend tätig, um die Ursache einzelner Ereignisse festzustellen,

---

<sup>2</sup> „Sicherheitsverletzung“ bezeichnet einen unberechtigten Zugriff, eine unberechtigte Offenlegung oder Verwendung personenbezogener Daten (PII), die die Sicherheit, Vertraulichkeit oder Integrität dieser Daten in einer Weise beeinträchtigt, dass diese Verwendung oder Offenlegung ein erhebliches Risiko eines finanziellen, Image-bezogenen oder sonstigen Schadens für die betroffene Person darstellt.

Trends bei mehreren Ereignissen über einen längeren Zeitraum zu erkennen und neue Strategien zu entwickeln, mit deren Hilfe ein erneutes Auftreten ähnlicher Vorfälle verhindert werden kann.

## **VII. Backup, Disaster Recovery (Notfallsystem) und Geschäftskontinuität**

OCLC hat ein Business Continuity Management System (BCMS), abgestimmt auf ISO 22301 und den Standards des United States National Institute of Standards and Technology sowie dem bundesdeutschen BSI Standard 100-5, eingeführt. OCLC unterhält ein weltweites Netz von Rechenzentren mit aktuellen Standorten in Dublin, Ohio, USA; Docklands, United Kingdom (Großbritannien); Toronto, Canada; und Sydney, Australien. OCLC verfügt über ein Hochverfügbarkeitssystem für WorldShare Management Services, WorldCat, WorldShare Interlibrary Loan, WorldCat Discovery und weiteren Diensten, für die OCLC verpflichtet ist, entsprechende Disaster Recovery (DR - Notfall) Funktionen vorzuhalten. OCLC kann durch seinen Disaster Recovery Standort (Notfallrechenzentrum) in Westerville, Ohio, USA die weltweiten Dienste jederzeit wiederherstellen und die Auswirkungen von Störungen minimieren. Lokale, sensible und nicht-bibliografische Daten werden in den jeweiligen lokalen Rechenzentren verwaltet, die die Bibliotheken in den jeweiligen geografischen Regionen versorgen (z.B. personenbezogene Daten in Europa werden im Rechenzentrum in der EU, in Docklands (Großbritannien) verarbeitet und gespeichert). Für Daten und Dienste, die in unseren regionalen Rechenzentren gehostet werden, hat OCLC Disaster Recovery Funktionen geschaffen um sie gegen die häufigsten Szenarien und Gefahren abzusichern. OCLC wählte die Rechenzentrumsstandorte, um die Wahrscheinlichkeit eines schweren Störfalles wegen Umweltgefahren und Naturkatastrophen zu minimieren. Zusätzlich verfügen die regionalen Rechenzentrenanbieter über Disaster Recovery Funktionen, die die Auswirkungen einer Katastrophe im physischen Rechenzentrum minimieren. Für den unwahrscheinlichen Fall eines katastrophalen Disaster Recovery Szenarios in einem der regionalen Rechenzentren, hat OCLC eine Standort Disaster Recovery Strategie um die Dienste rasch wieder herzustellen. Die Daten der Bibliotheken verbleiben in der gleichen geographischen Region, sind verschlüsselt, täglich gesichert (tägliche Datensicherung) und Datensicherungen werden wöchentlich zu einem externen aber regionalen Unternehmen zur Einlagerung von Datenträger verbracht.

## **VIII. Compliance**

### **A. Gesetzlicher Zugang zu Informationen**

OCLC befolgt zur Beantwortung von Informationsanfragen Dritter strikt rechtliche Verfahren. Daten können von Dritten nur auf dem Rechtsweg, etwa über Durchsuchungsbeschlüsse, Gerichtsbeschlüsse, Vorladungen, gesetzliche Ausnahmeregelungen, oder mit Einwilligung der Nutzer erlangt werden. Nach Eingang eines Antrags auf Offenlegung von Daten prüft die OCLC-Rechtsabteilung die Anfrage auf Übereinstimmung mit anwendbarem Recht. Ist die Anfrage rechtsgültig, benachrichtigt OCLC grundsätzlich den einzelnen Nutzer oder die Organisation, deren Daten angefordert werden, außer im Notfall oder soweit gesetzlich verboten.

### **B. Datenschutz**

Aufgrund des Charakters der OCLC WorldShare Services strebt OCLC die Einhaltung der strengsten Datenschutzgesetze und -verordnungen an und informiert sich laufend über Änderungen in aller Welt. Infolge dessen profitieren unsere Bibliothekskunden und deren Nutzer an Standorten wie den Vereinigten Staaten oft von der Einhaltung der anderswo geltenden umfassenderen Datenschutzgesetze durch OCLC.

OCLC stellt in Zusammenarbeit mit unseren Bibliotheksabonnenten die Einhaltung der jeweiligen lokalen, regionalen und nationalen Gesetze und Verordnungen sicher. OCLC verwendet personenbezogenen Daten, die es von den Bibliotheken oder Bibliotheksnutzern erhalten hat, nur soweit, wie dies von den Bibliotheken oder

Bibliotheksnutzern gestattet wurde oder anderweitig für die internen Zwecke von OCLC zur Erfüllung seiner Verpflichtungen im Rahmen verschiedener Verträge über OCLC-Dienste erforderlich ist.

OCLC wird personenbezogene Daten von Bibliotheksnutzern nicht ohne vorherige Zustimmung der Bibliothek oder der Bibliotheksnutzer verkaufen oder verteilen, vorausgesetzt, dass OCLC zur Offenlegung dieser Daten an folgende Empfänger berechtigt ist:

- eine Person, die gemäß anwendbaren Datenschutzgesetzen die Zugangsberechtigung zu diesen Daten besitzt;
- einen Dritten zum Zwecke der Erbringung der Dienste; und
- eine sonstige Person oder Behörde, die nach einem anwendbaren Gesetz berechtigt ist, Zugang zu diesen Daten zu verlangen.

Darüber hinaus wendet OCLC strenge übergeordnete Datenschutzgrundsätze an, um die Daten von Kunden und Endnutzern für alle seine Produkte und Dienstleistungen zu schützen. Diese Grundsätze werden auf <http://www.oclc.org/policies/privacy/> ausführlich erläutert. Die Datenschutzgrundsätze von OCLC heben keine Gesetze oder Verordnungen auf, die auf OCLC Anwendung finden, und setzen keine Vereinbarungen außer Kraft, die OCLC mit Kunden und Nutzern seiner Produkte und Dienstleistungen geschlossen hat.

## **IX. Schlussbemerkung**

OCLC hat sich verpflichtet, die in seinen Computersystemen gespeicherten Daten geschützt und sicher zu verwahren. OCLC setzt Kontrollen auf jeder Ebene von Datenspeicherung, -abruf und -übertragung ein. Bei OCLC können Bibliotheken und ihre Nutzer sicher sein, dass OCLC den Schutz, die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Daten für wichtig erachtet.